Energy efficient e-Healthcare system

M. Ajmal Sawand†, Najeed Ahmed Khan††, Abdul Rehman Soomrani† and Sheraz Ali†

† Sukkur Institute of Business Administration, Sukkur, Sindh, Pakistan
†† NED University of Engineering and Technology, Karachi, Pakistan

Abstract
With the development of internet of things, pervasive health monitoring has received lot of attention of the researchers and academia to make it more efficient and reliable. In this paper, we introduce efficient health-care monitoring system which leverages pervasive nature of the data transmission at the patient side as well as at clinical side. Furthermore, we define the efficient health-care monitoring system architecture and describe how to realize energy efficient medical data transmission among the participants (i.e., patients, doctors and health-care centers) to ensure the safety of different patients. We present health-care applications with supporting techniques and associated challenges with respect to energy efficient performance of the system and privacy of the stakeholders.

Key words:
Healthcare, Energy efficient

1. introduction

In Wireless Body Area Networks (WBAN), medical sensor equipped devices are leveraged to acquire conditions (vital signs) of the patients. Vital signs include heartbeat, temperature measurement, pulse monitoring etc. However, recent advancements in the WBAN network techniques have proved less costly and more flexible to scalability but it lacks efficiency with respect to the energy efficient performance, privacy and security. Since, growing usage of the Internet of Things (IoT) particularly increase in the usage of the smart-phones has created hindrances in the efficient communication in pervasive manner.

Recent advances in wireless body sensors and wireless communications have paved ways for the efficient health services to different types of the patients i.e., patients at high risk who suffer life threatening diseases. The medical sensors are generally attached with the human body either on the body or inside the body called implanted sensors which are dedicated to measure different health readings. In both situations either in hospitals or in remote areas. Since, pervasive use of smart homes and the wireless connectivity have facilitated patients as well as clinical staff to address the issues created by location and time (non-availability of the staff on particular time). Health monitoring system provides stable, reliable and consistent methodology to continuously collect related health data. Advancement in the communication technology has provided ways to move towards pervasive health-care instead of stay stucked on traditional clinical methods which are inefficient.

In this article, we envision a three layered health monitoring system architecture which include WBAN consisting of various bio-medical sensors, cloud layer which is responsible for providing privacy, security and data processing mechanism and clinical staff layer which enables pervasive nature of data transmission and collection. We will further highlight major service components and desirable properties of the proposed health monitoring system. In the corresponding section, we will discuss energy efficient data collection at the clinical side [1], [2].

2. health monitoring framework

Taking advantages of the modern communication technology, we have proposed a novel architecture for the health monitoring. In this architecture, there are three main stakeholders i.e., patients with medical sensors, doctors/hospitals and service provider. Proposed health care architecture can be characterized in three domains/layers as shown in Figure 1. Tier 1 carries various health related monitoring devices installed in or around the human body are integrated into (WBAN) [3]. Human being equipped with WBAN can remain at residence, in office, or in the clinic. Each sensor node in the WBAN can measure and calculate different readings. For instance, pulse monitoring sensor node will provide the pulse rate, location sensor will provide the co-ordinates of the exact location of the patient, and similarly ECG sensor displays signals related to the heartbeat of that particular human being.

The second tier encompasses controller personal server (PS) which could be a smart-phone, laptop or any desktop system [4]. The PS works as a controller of the various installed sensors which provides interface to the medical sensors, users and different types of the servers (which is somewhere in the cloud). PS also provides felicity to establish setup of a secure communication

Manuscript received April 5, 2017
Manuscript revised April 20, 2017

(key exchange), generally key exchange felicity is provided by the third party.

Once WBAN based eHealth system is configured, the PS application is responsible for overall management of the configured system, looking into the channel sharing, synchronization of the time, processing and transmission of the data. Once all this information is provided by the PS then application would be able to provide firsthand knowledge about the status of the patient's health. Very important point for our work is, whenever internet facility is available then PS need to establish a secure connection to the cloud where different medical servers are installed and transfers the all reports in related cloud. However, if transmission felicity is temporarily halted or link is down then in that condition PS is going to store the medical data provided by different medical sensors, later on it will resume uploading that particular data to the medical servers [7].

Tier three contains service layer which include medical servers, data storage, data processing and call center placed somewhere is the cloud. The service can issue recommendations, and even issue alerts (first aid, calling doctors/medical staff and ambulance etc.) if readings indicate the abnormal condition of the patient.

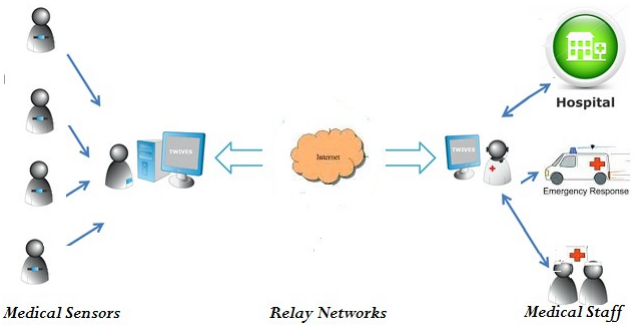

Fig. 1 Health Monitoring System Architecture

Figure 1: Health Monitoring System Architecture: (1) Patients equipped with medical sensors which transfer data to personal server/gateway (PDA / Smart-phone / Tablet PC). (2) Then, through any wireless connections (WiFi access point or 3G) medical data is transmitted to the cloud through internet connectivity (cloud or service center where different servers are installed and helpline for emergency directions to Doc- tor's/Ambulance Service/Hospitals etc.)

We can easily elaborate the idea of the health monitoring system from a simple example. For example, various patients and medical staff registered by the service provider's infrastructure (secure system which contains, database, authentication etc.) [1]. This infrastructure is quite scalable. Assuming that different patients enjoying their everyday life either in their homes or markets where third generation (3G) communication system and WiFi access points (free access either provided by city government or telephone service provider) are available everywhere. WBAN sends medical data either periodically or sporadic. Since, our proposed system also efficiently handles emergencies cases of the already registered patients. For example, one of the patients who is heart patient needs emergency during his shopping. Now there can be two scenarios:

(1) For instance, all medical sensors provide readings au- tomatically (periodically) to service provider whose servers (cloud services are hosted) and the (2) In this assumption, patients are not in critical condition they can calculate desired physiological readings from the medical sensors manually and transfer the data to the service provider. In both scenarios service provider is responsible to contact concerned doctor, hospital and ambulance service. Reports sent by the patient would contain the location information of the patient so that ambulance could catch him/her and moreover, staff in the hospital will prepare installation of the patient which ambulance will bring.

we are assuming that patient can manually calculate reading of his or her heartbeat, blood pressure, temperature etc. and sends to the cloud. Upon receiving this medical data of this particular patient, service provider will immediately pass that to the particular doctor and ambulance service center [10]. Moreover, service provider can communicate with doctor or hospital through personal mobile phone to avoid further delay. Within no time patient will receive emergency services and will be shifted to the hospital. Note: In this scenario, reports sent by patient manually or automatically will contain his/her location information through GPS sensor of the smart phone (Information about the location will be compulsory for the patients who are at high risk of heart attack etc.) [1]

Patients

Patient is the main stakeholder who will get the benefit from the system. There will be a unique ID of the patient and name/ID of his/her physician as well as names/IDs all spe- cialist doctors depending on his/her diseases. His/her medical history will be in the database of the service provider (cloud).

Registration Authority

Registration Authority will be present in the cloud which will provide secure/privacy preserved communication between patients and doctors/hospitals

and efficient security mechanism (transport layer security etc.) for the whole health monitoring system.

2.3 Heath-care Center

This entity of the health monitoring system is registered with complete physical address (GPS location), telephone numbers and availability of the doctors and it will periodically update the information about doctor's availability and their duty timings as well as number of standby doctors.

Doctor (Specialist/Physician): Doctors are registered with their home address and personal mobile number. They will keep updating about their private clinic timings and address of that place. Moreover, they will provide the list of their patients based on their conditions (normal, risk and high risk patients).

Ambulance Service: This part of the system gives com- plete updated information about the ambulance service (number of available ambulances and its first aid staff).

3. secure and efficient health-care system parameters

EHealth-care system design face many challenges, these challenges vary from efficiency to the security and trade- off between both. Efficient health-care system must be user friendly, it should be of reasonable size, ensure security/privacy of the users and efficient in performance etc. This paper contains the classification of technical as well as operational challenges.

Operational Challenges

Existing health-care systems are less user friendly for clinical staff as well as patients. Health-care systems need to be easy to use and which should also be scalable in case of the need. Since, health-care systems often require users to take their own measurements and send them to the data center, therefore systems should properties measuring the readings manually (users can also get readings whenever they need instead of waiting for the automated reading calculation based on the periodic time). Moreover, there can be critical situation of a user when he/she faces heart stroke or any other chronic disease, system should be capable of complying with the protocols and working mechanism of that particular sensing device. Efficient eHealth-care system need to be fully automated but rare involvement of the manual usage [2].

Technical Challenges

First and for most requirement of the efficient and secure health-care system is provide reliable data efficiently respecting the privacy of the all stakeholders. Below is the brief description of the problematic areas in designing efficient health-care system.

- Reliability: Sensor nodes are resource constraint, therefore most of the time these nodes produce false information due to different factors i.e., environmental hurdles as well as hardware operable problems. Moreover, wireless communication channels are already insecure and prone to problems and attacks. Challenges like, interference, path fading etc., are inherited from the wireless communication. Health-care systems deal with sensitive information which can lead to the life and death matters of the people, therefore inaccurate information and delay in its transmission may lead to the wrong diagnosis may results in loss of the life. Thus, health-care motoring framework needs to be reliable and efficient.
- Efficiency: The main hardware in the eHealth-care system is resource constraint i.e., battery, processing power and memory. Operating system, algorithms and applications in the sensor nodes should be energy-efficient so that these could ensure consistent monitoring. As these devices are attached with human body, the electromagnetic radiations generated by these medical devices should be minimized so that these harmful radiations could not provide adverse effects to the different human body parts. Most of the implanted medical sensors should be carefully installed and programmed so that these radiations could not damage in long run. Thus, efficient automated eHealth-care system needs to be developed with all these considerations and moreover, the trade-off between the efficiency and the security is very important factor which need to be balanced [2]
- Security and Privacy: Technological advancements in communication technology has paved ways for the pervasive nature of data transfer and collection but at the same time error-prone nature of the wireless communication channel has created security loopholes, taking advantage of that attackers may launch attacks. Various researchers have found the problems of node compromise which is important issue to be addressed at the priority. As health-care systems are designed for assistance in diagnosis and treatment of various diseases, security issues may render entire system unreliable, resulting lives of the human being at the risk. Moreover, health data is the most private data of the people therefore there should be fine grained

mechanism for accessing the patient's data. There is also need of the time to introduce well defined access privileges in the system so that no any concerned person could exploit his/her authority and misuse available medical data [8].

4. proposed solution

Our proposed framework is designed to minimize the energy consumption at personal server (by predicting its usage patterns) to efficiently upload the sensed data received from all the sensors of the wireless body area networks.

Energy consumption model in personal server

We propose framework of an efficient light weight scheme for uploading sensed data to the service domain/layer. As explained in the architecture, personal server is responsible for the sending data collected from the wireless body area networks. Personal server can be tablet pc, smart-phone, or personal data assistant. We assume that personal server can also use other applications like web browsing etc. which can put load on the bandwidth consumption. This usage pattern leads to the decrease in the energy utilization [9].

The purpose of suggested design is to predict how much energy is consumed at personal server by using different online applications (web browsing etc,). Suggested online.

Model is capable of personalization based on the needs of the usage patterns. Training occurs incrementally (success classifier weight is reduced, whereas failed classifiers weight is increased based on working of AdaBoost algorithm), each time internet applications are used.

Predictive internet applications usage features in personal server

We consider series of features proposed in prior studies [5], [6] that predict future application usage in the personal server of proposed health-care monitoring system (smart-phone/tablet pc). However, we do not consider those features exclude those features which consume lot of energy. Moreover, we consider the usage of the previous application, time and smart-phone usage state. day time usage of application is di- vided into four time intervals, each period of the time contains six hours (6am − 12pm, 12pm − 6pm, 6pm − 12am, 12am −6am). Similarly, the day of week is categorized into either weekend, or weekday [9].

Overview of the Adaptive Boosting Algorithm

Our solution is based on the machine learning algorithm called AdaBoost [11]. AdaBoost calls a weak classifier repeatedly in a series of T rounds {t = 1, ..., T }. For each call, a distribution of weights Dt is updated which indicates the importance of examples in the data set for the classification. After each round weight of the false classification is increased. Alternatively, the weights of each correctly classified example are reduced, so that the in the coming round new classifier looks for the falsely classified patterns.

Psedocode of AdaBoost

- *Input:* Learning sample E, Number of iterations T and a weak learner L.
- *Output:* A Global hypothesis H_T.
  for all *i from* 1 to m **do**
  $D_1(x_i) = 1/m$;
- **for all** *t from* 1 to T **do**
  $h_t = L(S,\mathbf{D}_t)$;
  $\epsilon_t = \sum x_i t.q.y_i \neq h_t(x_i)\ \mathbf{D}_t(x_i)$;

$$\alpha_t = \frac{1}{2}\ ln\ (\frac{1-\epsilon t}{\epsilon t}\ );$$

- **for all** *i from* 1 to m **do**
  $D_t + 1(x_i) =$

$$\frac{D_t(x_i).\exp(-\alpha_t y_i h_t(x_i))}{Z_t}$$

  where Z_t is normalization constant.
- $f(x) = \sum_{t=1}^{T} \alpha_t h_t(x)$;
  Return H_T such that
  $H_T(x) = sign\ (f(x))$

Adaboost is a machine learning algorithm for performing supervised learning [11]. Set of wrong/weak classifiers create the right classifier which is termed as strong learner. A weak learner is defined to be a classifier which is misclassified and it is considered as better than guessing. In contrast, a strong learner is a classifier that is termed as the correct classification. Most of the classification algorithms are consisting of iteratively weak classifiers with respect to distribution and resulting the correct/true/strong classifier. [12]

5. conclusion

This paper presented framework for the health care system which provides promising solution for the efficient uploading of sensed data collected from the wireless body area net- works. Presented eHealth-care monitoring system is designed to exploit opportunities

to transfer and upload at low energy cost (presented by everyday smart-phone/ tablet pc usage (i.e., personal server usage) medical data to the service center (cloud). We need to implement this framework in our future work to validate our proposed energy efficient design.

References

[1]. Sawand, S. Djahel, Z. Zhang and F. Nat-Abdesselam, "Toward energy-efficient and trustworthy eHealth monitoring system," in China Communications, vol. 12, no. 1, pp. 46-65, Jan. 2015

[2]. X. Liang et al., "Enabling pervasive healthcare through continuous remote health monitoring," in IEEE Wireless Communications, vol. 19, no. 6, pp. 10-18, December 2012.

[3]. D. He; S. Zeadally; N. Kumar; J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks With Provable Security," in IEEE Systems Journal , vol.PP, no.99, pp.1-12, April 2016.

[4]. N. Nasser and Yunfeng Chen, "Anytime and anywhere monitoring for the elderly," 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, Niagara Falls, ON, 2010, pp. 429-433.

[5]. T.-M.-T. Do and D. Gatica-Perez. "By their apps you shall understand them: mining large-scale patterns of mobile phone usage". In MUM '10.

[6]. C. Shin, J.-H. Hong, and A. K. Dey. "Understanding and prediction of mobile application usage for smart phones". In UbiComp '12.

[7]. Xu Li et al., "Smart community: an internet of things application," Communications Magazine, IEEE , vol.49, no.11, pp.68,75, November 2011

[8]. Jingwei Liu et al., "Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks," Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.2, pp.332,342, Feb. 2014

[9]. Nicholas D et al., "Piggyback CrowdSensing (PCS): energy efficient crowdsourcing of mobile sensor data by exploiting smartphone app op- portunities". In Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems (SenSys '13). ACM, New York, NY, USA, , Article 7 , 14 pages.

[10]. Ar Milenkovi et al., "Wireless sensor networks for personal health monitoring: Issues and an implementation" journal of Computer Com- munication 2006, volume 29 pages 2521-2533.

[11]. R.Meir, G.Ratsch: "An Introduction to boosting and Leveraging". In Machine Learning Summer School, pages 118-183. LNCS 2600, 2002

[12]. N. C. Oza and S. Russell. "Online bagging and boosting". In In Artificial Intelligence and Statistics 2001, pages 105112. Morgan Kaufmann, 2001.